UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JANE DOE, et al.

Plaintiffs,

v.

FULLSTORY, INC., et al.,

Defendants.

Case No. 23-cv-00059-WHO

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS; DENYING MOTION TO STRIKE

Re: Dkt. Nos. 138, 141

Plaintiffs allege that the defendants intentionally integrated their technologies on the platform of now-bankrupt website Hey Favor[1] in order to secure "personally identifiable information" ("PII") of users, including users' prescription information, answers to health questions, medications and side effects, allergies, age, and weight. TAC ¶ 13. Following prior motion practice and the filing of the Third Amended Complaint ("TAC"), only defendant FullStory, Inc. now moves to dismiss. Dkt. No. 138. It argues that this court lacks personal jurisdiction over it and that the TAC fails to state any claim against it.

Plaintiffs allege in the TAC that FullStory "intercepted ***all of the users' interactions*** on the Favor Platform (e.g., all individual clicks, keystrokes, and mouse movements), including their answers to highly sensitive medical questions." TAC ¶ 13 (emphasis in original). They assert (based on disclosures in the media and company complaints about FullStory) that FullStory ended up securing sensitive data from users despite the companies' efforts to prevent it from doing so.

[1] Hey Favor, Inc. ("Favor") (formerly the "Pill Club") is alleged to be "a combination telemedicine company and direct-to-consumer pharmacy that prescribes its patients birth control, emergency contraception (e.g., morning-after-pills), STI test kits, acne medicine, and prescription-strength retinol." Third Amended Complaint ("TAC") ¶ 1.

They contend that "FullStory understands that its software intercepts highly sensitive data, including health and medical information when used on a website or application like the Favor Platform, and that it would continue to do so as long as it remained installed" and that "FullStory did not take any steps to prevent Favor from using its technology on the Favor Platform or to prevent its interception and use of Favor users' sensitive health data —like answers to health questions to obtain birth control." *Id.* ¶¶ 54-58. These allegations are plausible and with one partial exception, state claims for relief. FullStory's motion to dismiss is DENIED.

DISCUSSION

I. PERSONAL JURISDICTION

In my January 2024 Order (Dkt. No. 115), I addressed FullStory's prior motion to dismiss for lack of personal jurisdiction.[2] Considering a then-new opinion, *Briskin v. Shopify, Inc.*, 87 F.4th 404, 412 (9th Cir. 2023), I concluded:

> Under *Briskin*, the requisite "forum-specific" focus for a "broadly accessible web platform" like FullStory cannot be established solely by allegations that FullStory knew it was processing the data of California-based consumers for a California-based merchant, here Favor. Something more is required.
>
> That something more is missing from the Amended Complaint. FullStory's motion to dismiss for lack of personal jurisdiction is GRANTED. Because *Briskin* clarified the nature of the personal jurisdiction test to be applied to a data processing platform like FullStory, plaintiff is given leave to amend to attempt to allege the something more that is required to satisfy the express aiming prong of the specific jurisdiction test.

Doe v. FullStory, Inc., No. 23-CV-00059-WHO, 2024 WL 188101, at *11 (N.D. Cal. Jan. 17, 2024). Relying on *Briskin* and my prior Order, FullStory moves again to dismiss, arguing that

[2] The Ninth Circuit employs a three-part test to determine whether there is specific jurisdiction over a defendant: (1) the non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws; (2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and (3) the exercise of jurisdiction must comport with fair play and substantial justice, *i.e.*, it must be reasonable. *Williams v. Yamaha Motor Co. Ltd.*, 851 F.3d 1015, 1023 (9th Cir. 2017); see *also Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004). To satisfy the first prong's "purposeful direction" test, plaintiffs must show that "the defendant ... (1) committed an intentional act, (2) expressly aimed at the forum state, (3) causing harm that the defendant knows is likely to be suffered in the forum state." *Schwarzenegger*, 374 F.3d at 803.

plaintiffs still fail to allege the "something more" to satisfy the "purposeful direction" prong of the applicable personal jurisdiction test.

Following my January 2024 Order and the completion of the briefing on this motion, the Ninth Circuit agreed to hear the *Briskin* case *en banc* and the panel opinion was vacated. *Briskin v. Shopify, Inc.*, No. 22-15815, 2024 WL 2148754, at *1 (9th Cir. May 14, 2024).[3] It is no longer persuasive authority.[4] Considering the pre-*Briskin* and post-*Briskin* cases, as well as the "something more" standard required by the now-vacated *Briskin* panel opinion, I find that plaintiffs have adequately alleged facts establishing personal jurisdiction over FullStory in this forum.

In the TAC, plaintiffs expanded on their jurisdictional allegations regarding FullStory:

> 65. FullStory's presence in California is significant and by all means intentional. Indeed, at all relevant times, FullStory targeted its provision and sale of session replay technology at California companies, including Favor, who maintain a website in California, as well as national websites that do business in California.
>
> 66. Not only does FullStory direct its business at California, but it actively sought out the benefits of the State and companies within it to assist with its collection and use of users' data. FullStory has created strategic partnerships with California-based companies to sell and implement FullStory's session replay software on its behalf in California as part of its "Partner Program." For instance, FullStory utilizes CXperts, a California-based company, as an "Elite" partner to help new FullStory clients complete the FullStory onboarding process. Likewise, it partners with Mentat Analytics, another California-based company, which provides consulting and optimization services to FullStory clients to create tags, events, and set up the FullStory dashboard and reports provided therein. Yet another California-based company FullStory relies on to provide its

[3] I also note that on the same day my January 2024 Order was issued, another judge in this District distinguished *Briskin* in a case very similar to this one. In that case, the Hon. Vince Chhabria found jurisdiction where "the alleged contracts between AddShoppers and California retailers are for the express purpose of enabling AddShoppers to collect customer data and conduct unsolicited customer outreach. In other words, the alleged agreements with California companies directly caused the harm." *McClung v. AddShopper*, Inc., No. 23-CV-01996-VC, 2024 WL 189006, at *1 (N.D. Cal. Jan. 17, 2024). Here, plaintiffs allege – as in *AddShopper* – that FullStory entered an agreement with California-based Hey Favor and other California companies to collect customer data and use that data to the detriment of consumers based in California and elsewhere. TAC ¶ 65.

[4] FullStory also asked me to stay the claims against it until the *en banc* opinion in *Briskin* is issued. Dkt. No. 149. I denied the motion to stay but allowed FullStory and plaintiffs to make further personal jurisdiction arguments in light of the vacated *Briskin* panel opinion. Dkt. No. 150.

> services is Sigma Infosolutions. FullStory advertises the services each of these California-based partners can provide on its website, each of which directs business to FullStory or helps incorporate its products for endclients. These partnerships are designed to, and do, further FullStory's sale and implementation of its session replay technology in California.
>
> 67. To further entrench itself in the California market, FullStory also integrates its services directly with the suite of products available in Google Cloud, a product created and operated by Google, LLC in California. FullStory is offered directly through the Google Cloud Marketplace operated by and from Google, LLC in California, where it can be made "more broadly available." FullStory's current employees, including executive officers, are based in California. FullStory's Chief Financial Officer, Edelita Tichepco, resides in San Francisco, California where she "oversee[s] all aspects of the company's financial operations." As are other pertinent personnel like FullStory's Senior Sales Engineer, Senior Marketing Operations Manager, and Head of Revenue Operations. So too are other employees, including an Enterprise Account Executive, Enterprise Sales Director, Onboarding Specialist, Commercial Account Director, Software Engineer, and Advisory Information Technology Specialist.

TAC ¶¶ 66-67 (footnotes omitted). Plaintiffs further identify significant Hey Favor employees based in California and allege that FullStory hosted or gave presentations at conferences in California to promote its services, and engaged in other specific acts soliciting and training clients on the use of the FullStory platforms in California. *Id*. ¶¶ 68-73.

The other significant addition to the TAC for the personal jurisdiction analysis is the addition of a California resident plaintiff, Jane Doe II. TAC ¶ 25. In my prior Order, I distinguished cases finding personal jurisdiction over FullStory and other session replay defendants given the lack of a California resident plaintiff here. *See Doe v. FullStory, Inc.*, 2024 WL 188101, at *11.

In light of these significant and material additions to the TAC, plaintiffs have satisfied the "purposeful direction" prong. They have plausibly alleged that FullStory committed an intentional act, expressly aimed at California, and that it knew would capture the health related PII of plaintiffs, including the California resident plaintiff. *See Herbal Brands, Inc. v. Photoplaza, Inc.*, 72 F.4th 1085, 1092 (9th Cir. 2023), *cert. denied*, 144 S. Ct. 693 (2024) ("But operating a website 'in conjunction with "something more"—conduct directly targeting the forum—is sufficient' to satisfy the express aiming prong.").

The types of conduct that plaintiffs allege FullStory intentionally took in California are related to its session replay software that allegedly harmed plaintiffs. That conduct included entering into a contract with the California-based business (*i.e.*, Hey Favor) and other California-based businesses that caused plaintiffs' harm, providing support services to clients for its session-replay software, soliciting sales of its session replay software through events in California, having employees based in California involved with the session replay software, and maintaining relationships with numerous partners based in California who help implement the session replay software. Purposeful direction has been satisfied.

FullStory argues that the numerous business contracts it is alleged to have with partners based in California and the numerous business contacts it is alleged to have conducted in California to promote its services are insufficient under *Briskin* and the pre-*Briskin* cases. Reply at 4; Supp. Brief [Dkt. No. 152] at 1-2. Unlike those cases, however, the contracts and contacts alleged here with partners in California are for the *exact* software that caused the harm alleged by plaintiffs (FullStory's session replay software that allegedly tracked plaintiffs' PII, including their sensitive health information).

The other opinions FullStory identified in its original motion and Supplemental Brief do not help them. For example, in *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503 (C.D. Cal. 2021), the only "suit-related contact" with the California forum was "that Plaintiff happened to be in California when he visited Nike's website." *Id.* at 513. Here, of course, Hey Favor was based in California, FullStory is alleged to have engaged in multiple instances of soliciting business through conferences in California, have made presentations in California, and have entered into client service agreements in California (including with Hey Favor). And at least one plaintiff is a California resident. Similarly inapposite is *Sacco v. Mouseflow, Inc.*, 2022 WL 4663361 (E.D. Cal. Sept. 30, 2022). There, the court found the "express aiming" required for personal jurisdiction was lacking where "Defendant did nothing specifically directed at California or California residents to tether it to this forum." *Id.* at *5. The *Sacco* court distinguished *S.D. v. Hytto Ltd.*, No. 18-CV-00688-JSW, 2019 WL 8333519 (N.D. Cal. May 15, 2019) because "the *Hytto* court determined the defendant was aware of its significant customer base in the forum, had

several partnerships with distributors in the forum, and knowingly placed its products in brick-and-mortar stores located in the forum. [] The FAC here is devoid of any similar allegations." *Id*. As noted above, plaintiffs here make those exact allegations with respect to FullStory.[5]

Given their plausibly alleged facts, plaintiffs have satisfied the purposeful direction prong. They have also satisfied the second prong of the personal jurisdiction test that their claim "arises out of or relates to the defendant's forum-related activities," since Hey Favor was based in California and at least one plaintiff lives in California. Defendants do not attempt to meet their burden on prong three, to show that exercise of personal jurisdiction over them would be not comport with fair play and substantial justice.

FullStory's motion to dismiss based on personal jurisdiction is DENIED.

II. CIPA

FullStory also moves to dismiss plaintiffs' claims under California Invasion of Privacy Act ("CIPA").[6]

A. Section 631

FullStory moves to dismiss the CIPA section 631 claim to the extent it is based on "wiretapping" because "Clause one of Section 631(a) [only] prohibits telephonic wiretapping, which does not apply to the internet." *Cody v. Ring LLC*, No. 23-CV-00562-AMO, 2024 WL 735667, at *3 (N.D. Cal. Feb. 22, 2024) (collecting cases); *see also Williams v. What If Holdings, LLC*, No. C 22-03780 WHA, 2022 WL 17869275, at *2 (N.D. Cal. Dec. 22, 2022) (determining "the first clause of Section 631(a) concerns telephonic wiretapping specifically and does not apply to the context of the internet").[7] Plaintiffs do not address clause one of Section 631(a) in their

---

[5] *Picot v. Weston*, 780 F.3d 1206 (9th Cir. 2015), is likewise inapposite. There, the defendant's allegedly tortious conduct was making statements while at his residence in Michigan to an Ohio resident that caused a Delaware corporation to cease making payments into trusts in Wyoming and Australia, without entering California, contacting any person in California, or otherwise reaching out to California. *Id*. at 1215.

[6] In the January 2024 Order, I dismissed the CIPA claim against FullStory with leave so that plaintiff could, at least, add "plausible facts to support application of California law to her claims and facts regarding FullStory's control of or possible use of end-users' captured data." *Doe v. FullStory, Inc.*, 2024 WL 188101, at *12.

[7] Cal. Penal Code §631 provides: (a) Any person who, by means of any machine, instrument, or

opposition. The claim under the clause one of Section 631 is DISMISSED with prejudice.

FullStory also argues that plaintiffs have failed to allege their claim under Section 631(a)'s second clause, penalizing attempts to willfully learn the contents of meaning of a communication in transit over a wire. FullStory contends that claim fails because any interception was permitted under Section 631's "party exception" and there was no "interception" of plaintiffs' communications.

1. Party Exception

If a party to a conversation uses a recording device to capture it, Section 631 is not violated. *See Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975) (explaining that Section 631 does not cover "participant recording"). There are two different lines of cases in this District addressing when a third-party like FullStory falls within the "party exception" to a conversation or recording between clients (*i.e.*, Hey Favor) and an end user (*i.e.*, plaintiffs).

Under the first line of cases, all that plaintiffs are required to allege is that the third-party defendant has the capacity to use the intercepted data for any purpose, even if that purpose is only analyzing its client's data. *See Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023) (sufficient as long as the third-party is alleged to have the capability of using the information secured, even without allegations of actual use); *see also Revitch v. New Moosejaw, LLC*, No. 18-CV-06827-VC, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019) ("Revitch adequately alleges that NaviStone acted as a third party that eavesdropped on his communications with Moosejaw because the code embedded into the Moosejaw.com pages functioned as a wiretap that redirected his communications to NaviStone while he browsed the site"); *Saleh v. Nike, Inc.*,

---

contrivance, or in any other manner, [1] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [2] who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [3] who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [4] who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

562 F. Supp. 3d 503, 520 (C.D. Cal. 2021) (third-party does not fall within the party exception as long as the third-party is capable of using the information).

Under the second line of cases, plaintiffs must plausibly allege that the third-party does more than simply analyze any intercepted data on behalf of its client (here Hey Favor), but also use the data somehow for its own ends. *See Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021); *see also Johnson v. Blue Nile, Inc.*, No. 20-CV-08183-LB, 2021 WL 1312771, at *2 (N.D. Cal. Apr. 8, 2021); *Yale v. Clicktale, Inc.*, No. 20-CV-07575-LB, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021); *Williams v. What If Holdings, LLC*, 22-cv-3780-WHA, 2022 WL 17869275 (N.D. Cal. Dec. 22, 2022) ("the question boils down to whether [defendant] was an independent third party hired to eavesdrop on [website owner's] communications, or whether [defendant's] software was merely a tool that [website owner] used to record its own communications with plaintiff."). As explained by the Hon. Jon S. Tigar recently in *Yockey v. Salesforce, Inc.*, 688 F. Supp. 3d 962 (N.D. Cal. 2023):

> If Salesforce can use its records of the communications for any purpose other than to furnish information relating to those communications to Kaiser, then it is more like the wife in *Ribas* who allowed Clark to eavesdrop. By contrast, if Salesforce "has no independent ability to divulge its recording for any other purpose but for that of" Kaiser, then it is more like the tape recorder in *Rogers*. *Id*.
>
> Plaintiffs allege that Chat "is run from Salesforce web servers," ECF No. 22 ¶ 12No. 22 ¶ 12, that communications over Chat are "routed through a Salesforce server," *id*. ¶ 13, that Salesforce "directly receives the electronic communications of visitors, *id*. ¶ 20, that Salesforce "analyzes the customer-support agent interactions in real time to create live transcripts of communications," *id*. ¶ 14, and that "supervisors can view transcripts in real time," *id*. ¶ 16. These allegations do not support a reasonable inference that Salesforce has the capability to use these communications for any purpose other than furnishing them to Kaiser. Chat, as alleged, is therefore more akin the tape recorder in *Rogers*, and Plaintiffs have thus failed to state a claim pursuant to Section 631.

Id. at []; *see also Cody v. Ring LLC*, No. 23-CV-00562-AMO, 2024 WL 735667, at *6 (N.D. Cal. Feb. 22, 2024) (adopting the "reasoning in *Javier*, and holds that a vendor hired by a website may act as a third-party eavesdropper if it secretly records conversations in real time" but also requiring plausible allegations that third-party has capability to use the recorded data for some purpose other than that of its client).

Another recent case, *Williams v. DDR Media, LLC*, No. 22-CV-03789-SI, 2023 WL 5352896, at *4 (N.D. Cal. Aug. 18, 2023) explained the split in as follows:

> This is a close question, and district courts have split on the issue. In *Graham v. Noom, Inc*., a district court considered similar allegations against Fullstory, a company that provides software that "records visitor data such as keystrokes, mouse clicks, and page scrolling" and enables clients to "see a 'playback' of any visitor's session." *Graham v. Noom, Inc*., 533 F. Supp. 3d 823 (N.D. Cal. 2021). The court held that Fullstory was not a third-party eavesdropper because it captured data only for the client website to use. The court reasoned that Fullstory "provides a tool – like the tape recorder in *Rogers* – that allows [a client website] to record and analyze its own data in aid of [the client website's] business." *Id*. at 832. Because there were no allegations that Fullstory "intercepted and used the data itself," the court concluded that it was not a third-party eavesdropper. *Id*. at 833. Other courts have followed *Graham's* reasoning. *See, e.g.*, *Williams v. What If Holdings, LLC*, No. C 22-03780 WHA, 2022 WL 17869275, at *3 (N.D. Cal. Dec. 22, 2022) (concluding that software vendor "functioned as a recorder, and not as an eavesdropper"); *Johnson v. Blue Nile, Inc*., No. 20-CV-08183-LB, 2021 WL 1312771, at *2 (N.D. Cal. Apr. 8, 2021).
>
> In *Javier v. Assurance IQ, LLC*, a district court took issue with this reasoning. *Javier v. Assurance IQ, LLC*, No. 20-CV-02860-CRB, 2023 WL 114225, at *6 (N.D. Cal. Jan. 5, 2023). It found that considering a software vendor's use of the information to determine whether it was a third-party eavesdropper "read[s] a use requirement into the second prong" of Section 631(a). Because the third prong of Section 631(a) separately penalizes use of information obtained via wiretapping, the court reasoned that considering use in analyzing the second prong would "add requirements that are not present (and swallow the third prong in the process)." *Id*. It also noted that the California Supreme Court did not consider the third party eavesdropper's "intentions" or "the use to which they put the information they obtained" in *Ribas v. Clark*, 38 Cal. 3d 355, 696 P.2d 637 (1985). The *Javier* court concluded that so long as the recording software provider has "the capability to use its record of the interaction for any other purpose," it is a third-party eavesdropper. *Id*.
>
> This is a difficult issue, and the *Javier* court's point that use is penalized by the third prong of the statute rather than the second is well-taken. However, the second prong of the statute penalizes anyone who "reads, or attempts to read, or to learn the contents or meaning of" the communication. Cal. Penal Code § 631(a). A person who eavesdrops on a conversation clearly falls under that definition. *And a software company that analyzes or uses a recorded communication has read, attempted to read, or learned the contents of that communication*. But the Court can think of no sense in which Jornaya has read, attempted to read, or learned the contents or meaning of the communication at issue here. Jornaya has merely recorded the communication for retrieval by a party to the same communication. Thus, the Court finds that Jornaya is more akin to a tape recorder vendor than an eavesdropper.

Id. at *4 (noting there was no allegations that defendant's product, TCPA Guardian, analyzed or otherwise manipulated the data).

In yet another recent discussion of the issue, *Smith v. Google, LLC*, No. 23-CV-03527-PCP, 2024 WL 2808270, at *4 (N.D. Cal. June 3, 2024), the Hon. P. Casey Pitts followed *Javier Assurance*: "Either way, the complaint alleges that the collected data is 'aggregated' and presented to Google Analytics customers in an online 'account dashboard.' Compl. ¶ 34. This suggests that Google processes and analyzes the data it collects at least to some extent. Even if this processing is done primarily for the benefit of Google Analytics users, Google is still the one 'reading' and/or 'using' the data it collects for the purposes of Section 631." *See also Valenzuela v. Nationwide Mut. Ins. Co*., No. 222CV06177MEMFSK, --- F.Supp.3d ---, 2023 WL 5266033, at *7 (C.D. Cal. Aug. 14, 2023) (following *Javier* line of cases in finding that the SaaS provider was a third party even if it did not use the data for its own independent purposes).

Here, even if there is a requirement that the third-party must be alleged to have processed, used, benefitted, or otherwise acted on the intercepted communications (as opposed to having the mere capacity to do so), plaintiffs satisfy that standard. Plaintiffs allege the following in the TAC:

> 136. FullStory "watch[es] sessions" through sophisticated session replay code that runs in the background of any given website or mobile application. Its session replay code makes a "detailed accounting of every action that takes place on [the] site or app. From mouse movements and clicks to screen swipes or typing." Each of these pieces of data are bundled, transmitted, and then "store[d] and organize[d]" by FullStory on their platform, along with a unique identifier (*i.e.*, UserID and SessionID) for each particular user whose communications they intercept.
>
> . . .
>
> 139. Once this data is intercepted, FullStory provides a dashboard platform that provides its clients "access [to] data that's automatically indexed, fully retroactive, and instrumentation-free to get insight into all digital interactions." On FullStory's dashboard, its clients are able to filter the sessions and identify users based on their actions on the site.
>
> 140. Not only does FullStory intercept vast amounts of data from its clients' websites, it also leverages that data to provide analytics insights such as factors impacting the sites conversions and device-specific bugs. It also supplies custom conversion analyses using its "extensive searchable data."
>
> 141.Recognizing the value and utility of this data, FullStory reserves the right to use this data to "monitor and improve [its] Services." It

> further states, "[f]or the avoidance of doubt" that it is granted the right to "use, reproduce and disclose" this data so long as it is purportedly "de-identified" for "product improvement" as well as any "other purposes" as it sees fit. This right survives the "termination" of agreements with FullStory clients.
>
> 142. FullStory's respective Data Processing Agreement with its customers states that FullStory may "share any Customer Data for cross-context behavioral advertising" so long as it obtains consent from the "Customer," *i.e.*, the business deploying its service, not the end user. It likewise states that it can "merge Customer Data with other data, or modify or commercially exploit any Customer Data" so long as the Customer agrees.
>
> 143. FullStory admits the same in its Privacy Policy, stating that it will use "aggregated" or purportedly "de-identified" data in its "discretion" including for "research, analysis, modeling, marketing, and improvement of [its] Services."
>
> 144. Even worse, not only does FullStory retain virtually all control over how it uses the data, but it further discloses the data to one of the largest advertisers in the world, Google, LLC. FullStory discloses end-user's data to Google for its own purposes, including "processing" and "storage" through Google's "BigQuery." FullStory also "sends data to Google" so that it can utilize "AI modeling and ML analytics." Upon information and belief, FullStory's transmittal of data to Google were the building blocks for the companies' consequential partnership for "Advanced Generative AI" announced in 2023.

These detailed allegations plausibly suggest that the data FullStory receives from its clients was analyzed by FullStory for its clients' use, but also that data is then leveraged and processed through AI and machine learning tools to provide more analytical insights to clients providing a benefit for FullStory itself *and* separately for clients. Also significant to this analysis, this is conduct that creates an even greater privacy risk.

FullStory argues that these allegations are insufficient. FullStory essentially takes the position that plaintiffs must allege that FullStory sold client data for its own uses to bring FullStory outside the party exception. That position goes too far. Even if FullStory primarily uses the intercepted data for its clients' purposes, there are additional plausible allegations that FullStory can and has used that intercepted data to improve its *own* analytics and services. Those allegations are supported by FullStory's Data Processing Agreement, which expressly preserves FullStory's right to use clients' data as it sees fit. Whether FullStory actually used its clients' data in these ways will be subject to discovery and tested at summary judgment. At this juncture, the

allegations suffice to defeat the party exception.

2. Interception

FullStory also argues that the Section 631 claim must be dismissed because plaintiffs failed to plausibly allege that FullStory "reads, or attempts to read, or to learn the contents" of plaintiffs' communications with Hey Favor while those communications were "in transit" as required by the second clause of Section 631. FullStory relies on a few very recent California district court cases addressing CIPA claims against FullStory or other session replay defendants. In *Love v. Ladder Fin., Inc.*, No. 23-CV-04234-VC, 2024 WL 2104497, at *2 (N.D. Cal. May 8, 2024), the Hon. Vince Chhabria of the Northern District dismissed a CIPA claim against FullStory because plaintiffs failed to allege facts supporting a CIPA claim under the second clause (violation where a person "willfully and without the consent of all parties to the communication ... reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit") or third clause (violation where a person "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained"). Judge Chhabria held:

> The plaintiffs cite FullStory's acknowledgement that it uses information collected from users of its customer websites for certain purposes, such as security, legal compliance, and service improvement. Additionally, FullStory states that it "may use and share information in an aggregated and de-identified manner at [its] discretion, including for research, analysis, modeling, marketing, and improvement of our Services." But none of that makes it plausible that FullStory is accessing or reading the personal identifying information or sensitive health information entered into the form. There is no coherent story of how or why FullStory would learn such granular information about users of one if its customers' sites—information that has nothing to do with its alleged service or stated uses of consumer data. Merely quoting these lines from the policy and then making broad assertions about use is not enough to state a claim under the second clause of § 631(a).
>
> The claim under the third clause fails for similar reasons. The third clause makes it a violation when a person "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained." The third clause references the second clause. If someone violates CIPA by learning the contents of a communication in a proscribed manner, then someone who uses or shares the ill-gotten contents of that communication also violates CIPA. But, as discussed, there is no plausible allegation that FullStory learned what the users wrote in the insurance quote forms. Similarly,

> there is no plausible allegation that FullStory uses the personal information in those forms. Thus, the plaintiffs have failed to sufficiently allege that FullStory violated the third clause of § 631(a).

Love, 2024 WL 2104497, at *2; *see also James v. Allstate Ins. Co.*, No. 3:23-CV-01931-JSC, 2023 WL 8879246, at *3 (N.D. Cal. Dec. 22, 2023) ("Plaintiff has [] not alleged Heap read, attempted to read, or to learn the meaning of his communications with Allstate; rather, he merely alleges Heap recorded the data and stores it on its servers. [] Plaintiff's allegation that 'this data is stored or can be accessed by Heap' is insufficient to support a plausible interference Heap attempted to read or learn the contents of the communication while in transit") (internal citations omitted); *Williams v. DDR Media, LLC*, No. 22-CV-03789-SI, 2023 WL 5352896, at *4 (N.D. Cal. Aug. 18, 2023) (because the second clause of Section 631 "penalizes anyone who 'reads, or attempts to read, or to learn the contents or meaning of' the communication," clause two does not cover a software company that "merely recorded the communication for retrieval by a party to the same communication").

However, as discussed above, plaintiffs here allege that FullStory does more than simply record information for retrieval by its clients like Hey Favor. Plaintiffs assert that FullStory organizes the data, analyzes the data, and presents the data in ways that allow clients to "identify users based on their actions on the site." *See, e.g.*, TAC ¶ 139. They also contend that FullStory does this not only for its clients' needs but also for its own ends. *Id.* ¶¶ 140-141. Plaintiffs' allegations of interception are sufficient to state the Section 631 claim.

B. Section 632

FullStory argues that the claim under Section 632 of CIPA, penalizing intentional use of an "electronic amplifying or recording device" to eavesdrop upon or record a "confidential communication," fails because plaintiffs do not allege facts plausibly supporting FullStory's *intentional* acquisition of a confidential communication. To support its argument, FullStory notes that plaintiffs admit – citing FullStory's Data Use Policy – that FullStory "requires users to block sensitive information from being recorded" (although plaintiffs also assert FullStory "does not have the capability to do so and does not enforce that policy."). TAC ¶ 145. FullStory argues that it is contradictory for plaintiffs to allege that it collected sensitive data from Hey Favor users while

admitting that its policy required Hey Favor to block the same. Moreover, given its policy, FullStory contends that at most its collection of any sensitive data was accidental and not intentional. *See Lozano v. City of Los Angeles*, 73 Cal. App. 5th 711, 728 (2022), *review denied* (Apr. 20, 2022) ("'Penal Code section required an intent to record a confidential communication, rather than simply an intent to turn on a recording apparatus which happened to record a confidential communication.'" (quoting *Estate of Kramme*, 20 Cal.3d 567, 572, fn. 5 (1978)).[8]

But plaintiffs allege that FullStory knew it did not have the capability to block sensitive information and did not enforce that policy. TAC ¶ 145. They also rely on the reasonable inference that FullStory knew that sites like Hey Favor were focused on the provision of healthcare services and products, and that by selling its session replay software with its promise to track every action that takes place on a client's website (TAC ¶ 136) to customers like Hey Favor, FullStory knew that it would be receiving, processing, and analyzing sensitive health care information and intended to do so. Plaintiffs' allegations will be subject to discovery and tested on summary judgment, but they are adequate at this juncture. *See Lopez v. Apple, Inc*., 519 F. Supp. 3d 672, 689 (N.D. Cal. 2021) (intent alleged for Section 632 where "plaintiffs adequately allege that Apple knew of the accidental Siri triggers, and the Court finds it plausible that some of those triggers would, with 'substantial certainty,' occur in confidential contexts"); *see also Doe v. Meta Platforms, Inc*., No. 22-CV-03580-WHO, 2023 WL 5837443, at *7 (N.D. Cal. Sept. 7, 2023 ("Whether Meta's affirmative disclosures and back-end filtering process sufficiently negate intent

[8] In its motion, FullStory asks me to take judicial notice of the full contents of documents it contends are incorporated by reference in plaintiffs' TAC. *See* Dkt. No. 138-1, Declaration of Matthew Q. Verdin. Plaintiffs object and move to strike three of those exhibits (Dkt. No. 141): (1) Ex. A, the FullStory Data Processing Agreement (quoted in TAC ¶¶ 73, 142, 144); (2) Ex. C, the FullStory Terms and Conditions from June 2020 (quoted in TAC ¶ 141); and (3) Ex. D, the FullStory Privacy Policy from March 22, 2024 (quoted in TAC ¶¶ 143, 176). Plaintiffs contend these documents cannot be judicially noticed because plaintiffs' reliance on them is not central to their claims and even if noticeable, cannot be used to dispute the merits of plaintiffs' allegations. The motion to strike is GRANTED in part. Each of the exhibits are substantively relied on by plaintiffs and central to their CIPA claim to plausibly support the inference that FullStory uses or has the capability to use consumer data for its clients' or its own purposes, so I will take judicial notice of them. I will not rely on the sections of those documents identified by FullStory – that according to defendant prevents some uses of the data without customer consent – to foreclose any of plaintiffs' claims. How FullStory implemented the various provisions of its policies, and what sorts of consents Hey Favor provided, will be subject to discovery.

depends on Meta's knowledge as well as its implementation and the efficacy of its alleged contractual efforts and back-end filtering. Those will be tested on an evidentiary record.").

C. Extraterritoriality

On its prior motion to dismiss, FullStory squarely raised the argument that California law should not apply to the then-sole plaintiff who resides in Arkansas, in light of FullStory's residence in Georgia as well as the absence of allegations regarding terms of service that would impose California law on that plaintiff's claims. January 2024 Order at 20. In light of the dismissal with leave to amend (based on the need to add more personal jurisdiction allegations), I did not address the issue. *Id*. FullStory re-raises its choice-of-law argument on this motion. MTD at 17-21 (arguing "at a minimum" the CIPA claims brought by the Arkansas Doe plaintiff should be dismissed).

The posture of this case today is significantly different than it was in January, with the addition of the California Doe resident. In light of the strong allegations connecting FullStory's conduct to California, sufficient to establish personal jurisdiction over FullStory, and given the California resident Doe, I will defer the choice-of-law challenge until discovery concerning how and where FullStory accessed, processed and/or stored plaintiffs' data is conducted. *See, e.g., Kellman v. Spokeo, Inc.*, 599 F. Supp. 3d 877, 894 (N.D. Cal. 2022), *motion to certify appeal denied*, No. 3:21-CV-08976-WHO, 2022 WL 2965399 (N.D. Cal. July 8, 2022) (noting that some courts "decide choice-of-law issues this early in the case but often defer them until class certification," especially where discovery is meaningful to the choice-of-law inquiry); *see also Doe v. Meta Platforms, Inc.*, No. 22-CV-03580-WHO, 2023 WL 5837443, at *6 (N.D. Cal. Sept. 7, 2023) (deferring choice of law analyses where discovery will confirm the nexus to California and where plaintiffs had plausibly alleged "the conduct at issue, in terms of the design and marketing of the [tracking] technology and development and implementation" occurred in California).

In arguing that the choice of law issue concerning the Arkansas Doe should be decided now, FullStory relies on *Doe v. Kaiser Found. Health Plan, Inc.*, No. 23-CV-02865-EMC, 2024 WL 1589982 (N.D. Cal. Apr. 11, 2024). But there, "the Court compelled John Doe, the only

California Plaintiff, to arbitration. As a result of that ruling, the first issue the Court must address is choice of law, i.e., whether CIPA (a California law) can apply to all Plaintiffs and all putative class members regardless of their residence." *Id.* at *11. That is not the case here. Similarly inapposite is *Katz-Lacabe v. Oracle Am., Inc.*, No. 22-CV-04792-RS, 2023 WL 6466195, at *3 (N.D. Cal. Oct. 3, 2023), aff'd, No. 22-CV-04792-RS, 2023 WL 7166815 (N.D. Cal. Oct. 30, 2023). There, considering the application of California law to a nationwide class, the court determined "that California law does not apply nationwide for Plaintiffs' intrusion upon seclusion claim. Therefore, Plaintiffs' intrusion upon seclusion claim—to the extent it is brought on behalf of the United States Class under California law, as opposed to solely on behalf of the California Sub-Class—is dismissed without leave to amend." *Id.* at *3. On this motion, FullStory did not move to strike any class allegations and I do not reach whether it is appropriate to apply California law to a nationwide class.[9]

As recognized by the California Supreme Court considering CIPA, discovery will show whether FullStory intercepted both Does' healthcare information in California (given Hey Favor's location in California) or whether the interception of the Arkansas Doe's information by FullStory occurred outside of or otherwise had little connection to California. *See Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 119 (2006) ("Interpreting that statute to apply to a person who, while outside California, secretly records what a California resident is saying in a confidential communication while he or she is within California, however, cannot accurately be characterized as an unauthorized extraterritorial application of the statute, but more reasonably is viewed as an instance of applying the statute to a multistate event in which a crucial element—the confidential communication by the California resident—occurred in California. The privacy interest protected by the statute is no less directly and immediately invaded when a communication within California is secretly and contemporaneously recorded from outside the state than when this action

[9] For this reason, FullStory's other cases are inapposite. *See, e.g., James v. Walt Disney Co.*, No. 23CV02500EMCEMC, 2023 WL 7392285, at *18 (N.D. Cal. Nov. 8, 2023), motion to certify appeal denied, No. 23CV02500EMCEMC, 2024 WL 664811 (N.D. Cal. Feb. 16, 2024) ("Plaintiffs' concession that a nationwide class is not possible, the Court grants Disney's motion for relief. The nationwide class is dismissed and/or stricken.").

occurs within the state. A person who secretly and intentionally records such a conversation from outside the state effectively acts within California in the same way a person effectively acts within the state by, for example, intentionally shooting a person in California from across the California–Nevada border.").

Other than the CIPA claim based on clause one of section 631(a), FullStory's motion to dismiss the CIPA claims is DENIED.

III. INTRUSION ON SECLUSION

FullStory argues that plaintiffs' intrusion on seclusion claim fails because plaintiffs have not adequately alleged that FullStory intentionally intercepted their sensitive healthcare data or otherwise engaged in "highly offensive" behavior. These arguments are foreclosed by the discussion above (regarding intent) as well as by my applicable conclusions in the January 2024 Order. *See* January 2024 Order at 10-11 (discussing allegations regarding interception of sensitive medical treatment information); *see also Doe v. Regents of Univ. of California*, 672 F. Supp. 3d 813, 820 (N.D. Cal. 2023) ("Personal medical information is understood to be among the most sensitive information that could be collected about a person, and I see no reason to deviate from that norm."). The motion to dismiss the intrusion claim is DENIED.

IV. UNJUST ENRICHMENT

FullStory argues that any unjust enrichment claim fails because the substantive claims fail. However, plaintiffs' CIPA claims survive. FullStory's motion to dismiss the unjust enrichment claim is DENIED.

V. STANDING FOR INJUNCTIVE RELIEF

Finally, FullStory argues plaintiffs lack standing to seek injunctive relief against FullStory because their harm – FullStory's interception of their data through their use of Hey Favor's website – is not likely to occur in the future given Hey Favor's Chapter 11 bankruptcy and its dba PillClub "transitioning patent care to Nurx." MTD at 23 n. 9. FullStory also argues that given plaintiffs' knowledge that Hey Favor was using FullStory's session replay services, it would not be likely to use those services again.

This ignores plaintiffs' allegations that FullStory continues to have possession of plaintiffs'

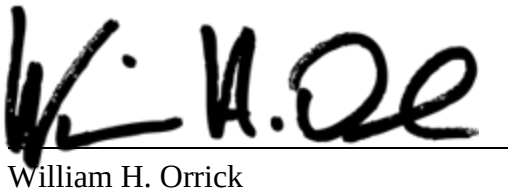
healthcare information. TAC ¶¶ 23, 30, 136-137. There is a reasonable inference that FullStory continues to and may use that information in the future, necessitating injunctive relief if plaintiffs prevail on their claims. At this juncture, therefore, plaintiffs have standing to pursue a claim for injunctive relief.

CONCLUSION

FullStory's motion to dismiss for lack of personal jurisdiction and for failure to state a claim is DENIED, except for the claim under the first clause of Section 631(a).

IT IS SO ORDERED.

Dated: July 17, 2024



William H. Orrick
United States District Judge